POST-BREACH CONSUMER TIPS

Data breaches pose a potential risk to consumers in the form of identity theft, account takeover, and fraud when personal and sensitive information is compromised.

We encourage you to follow these tips following a breach that has exposed personal information. These tips are a good way to minimize the risk or impact of data breaches.

CREDIT REPORTS

If any portion of your Social Security Number was compromised, you should consider ordering a credit report and closely review it.

You may want to consider placing a security freeze on your credit report. A **security freeze**, also referred to as credit freeze, can protect you by restricting access to your credit report. During a freeze, the credit union, along with other financial institutions or lenders, are blocked from ordering a credit report unless a pre-set PIN is provided to lift the freeze.

You will have to allow for extra time for a loan or credit approval after placing a freeze. Members will have to request the security freeze from each credit bureau – Equifax, Experian, TransUnion, and Innovis.

In some states, the credit bureau charges a fee to freeze, temporarily thaw, and/or unfreeze a credit report.

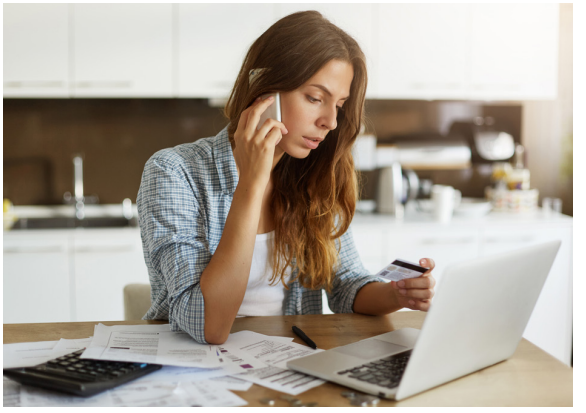
FRAUD ALERTS

Place a fraud alert on your credit report if you are a victim of identity theft. When a financial institution or lender pulls a credit report containing a fraud alert, they are required to call the phone number contained in the alert, or use other reasonable means to verify it was actually you that applied for an account or loan.

Verify how long the initial fraud alert remains on your credit report and when it must be renewed.

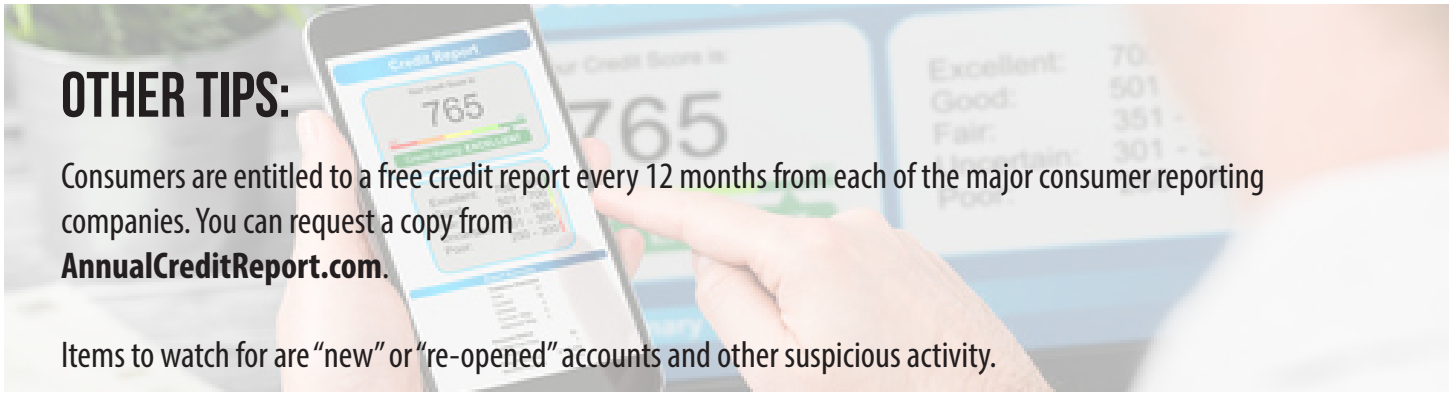
FRAUDULENT BANK ACCOUNTS

Although you can freeze your credit report to prevent inquiries and new loans from being granted, criminals may still be able to open a new deposit account in your name if your personal information is known to others. This can happen in a number of ways including breaches, such as the large one that occurred in 2017, which disclosed personal information on millions of consumers.



ChexSystems is a nationwide consumer reporting agency that gathers information on closed checking and savings accounts from their clients. This information may then be used by other financial institutions when someone applies to open a checking or savings account.

If you believe you have been a victim of identity theft or if you would like to get a copy of your Consumer Disclosure Report to see who may have pulled your ChexSystems report for any reason, visit www.chexsystems.com. The site provides instructions on how to obtain your report as well as valuable information on how to place a security alert or security freeze on your information.



OTHER TIPS:

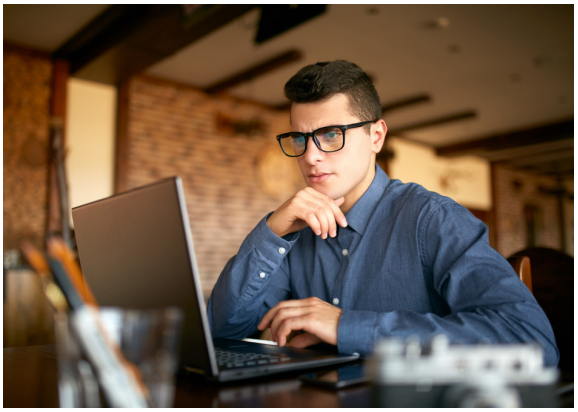
Consumers are entitled to a free credit report every 12 months from each of the major consumer reporting companies. You can request a copy from **AnnualCreditReport.com**.

Items to watch for are "new" or "re-opened" accounts and other suspicious activity.

ONLINE LOGIN OR PASSWORD INFORMATION

If any of your online login or password information was compromised, you should:

- Log in to the member account as soon as possible and change the login and password.
- Make changes to accounts that use the same logins and passwords for multiple sites.
- Always use strong passwords that are at least 11 characters in length that are case-sensitive and include alpha-numeric characters and at least one symbol.
- Use a password checker to ensure a strong password was implemented.



DEBIT OR CREDIT CARD INFORMATION

If a debit or credit card information was compromised:

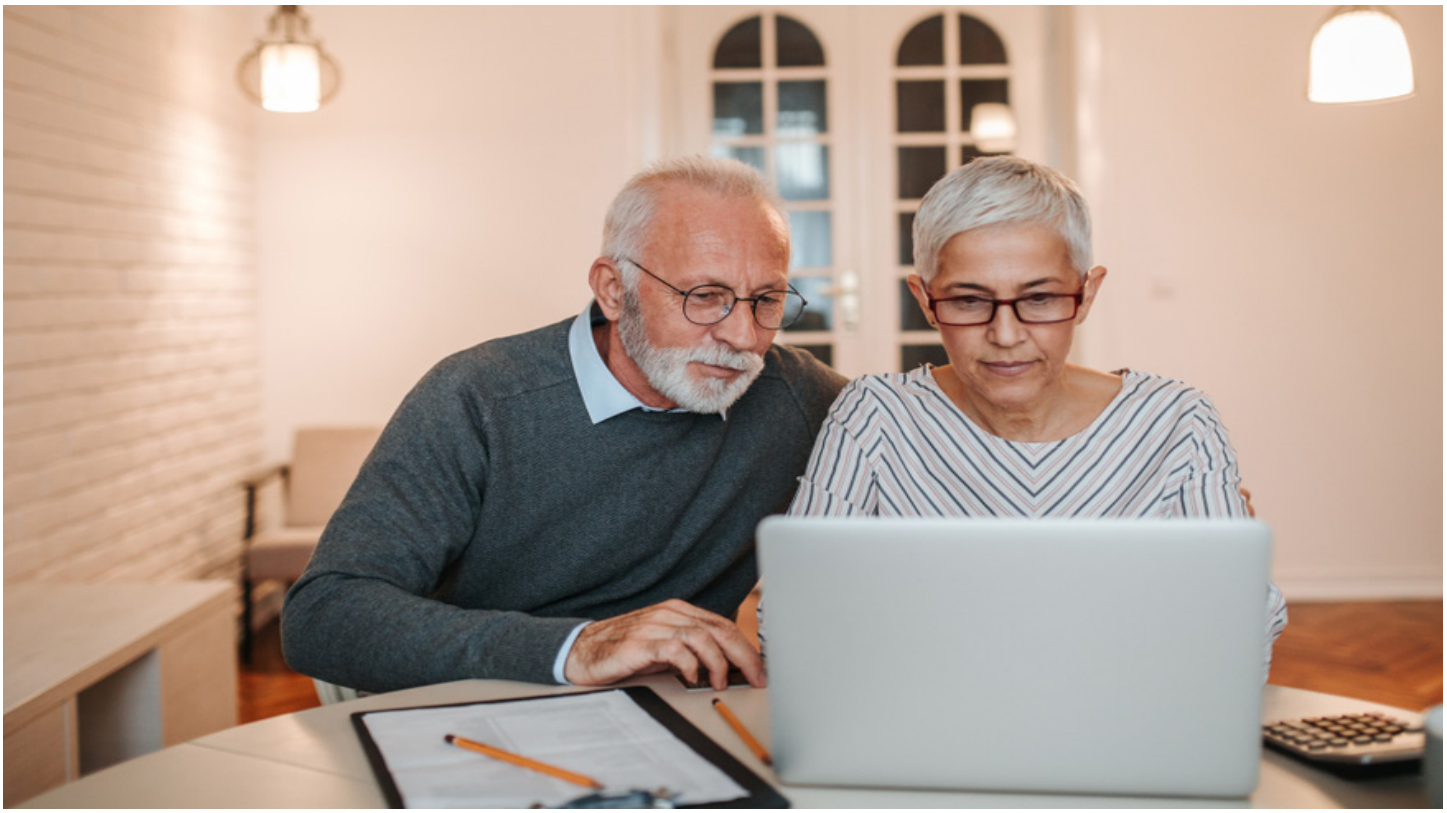
- Call the credit union/financial institution and request the old card to be canceled and request a new one.
- Review account activity and report any unauthorized transactions on a timely basis.

CREDIT UNION/FINANCIAL INSTITUTION ACCOUNT INFORMATION

If credit union/bank account information was compromised:

- Review account activity and report any unauthorized transactions.
- Consider closing the account and request a new one, but be mindful of potential delays and interruptions to any automatic payments or deductions.

PROTECT YOURSELF FROM SCAMS



• Be mindful of emails or phone requests claiming to be from the business or financial institution which was breached.

Phishing emails often contain attachments or links to malicious websites infected with malware. Avoid opening attachments and clicking on links contained in emails received from unfamiliar sources.

• Be wary of SMiSHing attacks which are similar to phishing but in SMS text messages. Avoid clicking on links or calling the telephone number contained within text messages received from unfamiliar sources.

• To avoid tax identity fraud make a point of filing annual tax returns promptly.

Should you be notified that more than one return was filed in your name; you owe additional tax; or that records indicate that earnings were more than the amount of wage reported, complete an IRS Identity Theft Affidavit form 14039, and contact the IRS Identity Protection Specialized Unit at 800.908.4490.

• Check with the credit union/financial institution for additional account protections such as security challenge pass-phrase, account notes, and travel protections.

• In general, you should be wary of offers that are too good to be true, require fast action, or instill a sense of fear.